

#5

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant: Junya WATANABE      Examiner: Unassigned  
Serial No.: 09/960,424      Group Art Unit: Unassigned  
Filed: September 21, 2001      Docket: 14944  
For: DIGITAL CONTENTS GENERATING  
APPARATUS AND DIGITAL CONTENTS  
REPRODUCING APPARATUS      Dated: October 10, 2001

Assistant Commissioner for Patents  
Washington, DC 20231

**CLAIM OF PRIORITY**

Sir:

Applicant in the above-identified application hereby claims the right of priority in connection with Title 35 U.S.C. §119 and in support thereof, herewith submits a certified copy of Japanese Patent Application 2000-286640 (286640/2000), filed on September 21, 2000.

Respectfully submitted,

Paul J. Esatto, Jr.  
Registration No. 30,749

Scully, Scott, Murphy & Presser  
400 Garden City Plaza  
Garden City, NY 11530  
(516) 742-4343  
PJE:ahs

**CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner of Patents and Trademarks, Washington, D.C. 20231 on October 10, 2001.

Dated: October 10, 2001

Janet Grossman



日本国特許庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application: 2000年 9月21日

出願番号

Application Number: 特願2000-286640

出願人

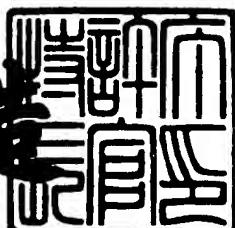
Applicant(s): 日本電気株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 7月27日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3067119

【書類名】 特許願

【整理番号】 68501847

【あて先】 特許庁長官殿

【国際特許分類】 H04N 11/04

【発明者】

【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

【氏名】 渡辺 淳也

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100082935

【弁理士】

【氏名又は名称】 京本 直樹

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100082924

【弁理士】

【氏名又は名称】 福田 修一

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100085268

【弁理士】

【氏名又は名称】 河合 信明

【電話番号】 03-3454-1111

【手数料の表示】

【予納台帳番号】 008279

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9115699

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタルコンテンツ生成装置及び再生装置

【特許請求の範囲】

【請求項1】 デジタルコンテンツに電子透かしデータを挿入するデジタルコンテンツ生成装置において、

前記電子透かしデータと所定のIPアドレスとに基づいて暗号キーを生成する暗号キー生成部と、前記暗号キーを用いて、前記電子透かしデータが挿入されたデータを暗号化し、通信ネットワークに出力する暗号化部と、前記通信ネットワークから入力した電子透かしデータとIPアドレスとに基づいて、前記暗号化されたデータを復号するための復号キーを生成し、前記通信ネットワークに出力する復号キー生成部とを備えることを特徴とするデジタルコンテンツ生成装置。

【請求項2】 デジタルコンテンツを離散コサイン変換することによりDCT係数を生成する離散コサイン変換部と、電子透かしデータを前記DCT係数に足しこむ電子透かし挿入部とを備えるデジタルコンテンツ生成装置において

前記電子透かしデータと所定のIPアドレスとに基づいて暗号キーを生成する暗号キー生成部と、前記暗号キーを用いて、前記電子透かしデータが挿入されたデータを暗号化し、通信ネットワークに送出する暗号化部と、前記通信ネットワークから入力した電子透かしデータとIPアドレスとに基づいて、前記暗号化されたデータを復号するための復号キーを生成し、前記通信ネットワークに出力する復号キー生成部とを備えることを特徴とするデジタルコンテンツ生成装置。

【請求項3】 前記暗号化部は、前記暗号化されたデータをデータ記憶媒体に格納することを特徴とする請求項1又は2に記載のデジタルコンテンツ生成装置。

【請求項4】 電子透かしデータが挿入されたデジタルコンテンツから電子透かしデータを検出するとともに、当該デジタルコンテンツを表示手段に表示するデジタルコンテンツ再生装置において、

電子透かしが挿入され、かつ、暗号化されたデジタルコンテンツを通信ネットワークから入力し、当該デジタルコンテンツから電子透かしデータを検出す

る電子透かしデータ検出部と、復号キーを用いて前記暗号化されたディジタルコンテンツを復号する復号化部と、前記復号化部の出力を再生し、前記表示手段に出力する再生部と、前記検出した電子透かしデータと所定のIPアドレスとを前記通信ネットワークに出力し、前記復号キーを前記通信ネットワークから入力するネットワークインターフェース部とを備えることを特徴とするディジタルコンテンツ再生装置。

【請求項5】 電子透かしデータが挿入されたディジタルコンテンツから電子透かしデータを検出するとともに、当該ディジタルコンテンツを表示手段に表示するディジタルコンテンツ再生装置において、

電子透かしが挿入され、かつ、暗号化されたディジタルコンテンツを通信ネットワークから入力し、当該ディジタルコンテンツから電子透かしデータを検出する電子透かしデータ検出部と、復号キーを用いて前記暗号化されたディジタルコンテンツを復号する復号化部と、前記復号化部の出力を逆離散コサイン変換する逆DCT部と、前記逆DCT部の出力を再生し、前記表示手段に出力する再生部と、前記検出した電子透かしデータと所定のIPアドレスとを前記通信ネットワークに出力し、前記復号キーを前記通信ネットワークから入力するネットワークインターフェース部とを備えることを特徴とするディジタルコンテンツ再生装置。

【請求項6】 前記電子透かし検出手段は、電子透かしが挿入され、かつ、暗号化されたディジタルコンテンツをデータ記憶媒体から入力することを特徴とする請求項4又は5に記載のディジタルコンテンツ再生装置。

【請求項7】 通信回線と、該通信回線と相互に接続されたディジタルコンテンツ生成装置とディジタルコンテンツ再生装置とを備えたシステムにおいて、

前記ディジタルコンテンツ生成装置は、ディジタルコンテンツに電子透かしデータを挿入する電子透かし挿入部と、前記電子透かしデータと所定のIPアドレスとに基づいて暗号キーを生成する暗号キー生成部と、前記暗号キーを用いて、前記電子透かしデータが挿入されたデータを暗号化して前記通信回線に出力する暗号化部と、前記通信回線から入力した電子透かしデータとIPアドレスとに基づいて、前記暗号化されたデータを復号するための復号キーを生成し、前記通信

ネットワークに出力する復号キー生成部とを備え、

前記ディジタルコンテンツ再生装置は、前記暗号化されたデータを前記通信回線から入力し、当該データから前記電子透かしデータを検出する電子透かしデータ検出部と、前記復号キーを前記通信回線から入力し、当該復号キーを用いて前記暗号化されたデータを復号する復号化部と、前記復号化部の出力を再生し、前記表示手段に出力する再生部と、前記検出した電子透かしデータと所定のIPアドレスとを前記通信回線に出力することを特徴とするディジタルコンテンツ提供システム。

【請求項8】 通信回線と、該通信回線と相互に接続されたディジタルコンテンツ生成装置とディジタルコンテンツ再生装置とを備えたシステムにおいて、

前記ディジタルコンテンツ生成装置は、ディジタルコンテンツに電子透かしデータを挿入する電子透かし挿入部と、前記電子透かしデータと所定のIPアドレスとに基づいて暗号キーを生成する暗号キー生成部と、前記暗号キーを用いて、前記電子透かしデータが挿入されたデータを暗号化してデータ記憶媒体に出力する暗号化部と、前記通信回線から入力した電子透かしデータとIPアドレスとに基づいて、前記暗号化されたデータを復号するための復号キーを生成し、前記通信ネットワークに出力する復号キー生成部とを備え、

前記ディジタルコンテンツ再生装置は、前記暗号化されたデータを前記データ記憶媒体から入力し、当該データから前記電子透かしデータを検出する電子透かしデータ検出部と、前記復号キーを前記通信回線から入力し、当該復号キーを用いて前記暗号化されたデータを復号する復号化部と、前記復号化部の出力を再生し、前記表示手段に出力する再生部と、前記検出した電子透かしデータと所定のIPアドレスとを前記通信回線に出力することを特徴とするディジタルコンテンツ提供システム。

【請求項9】 ディジタルコンテンツに電子透かしデータを挿入する処理を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体において、

前記電子透かしデータと所定のIPアドレスとに基づいて暗号キーを生成する処理と、前記暗号キーを用いて、前記電子透かしデータが挿入されたデータを暗号化し、通信ネットワークに出力する処理と、前記通信ネットワークから入力

した電子透かしデータとIPアドレスに基づいて、前記暗号化されたデータを復号するための復号キーを生成し、前記通信ネットワークに出力する処理とを実行するためのプログラムを記録した記録媒体。

【請求項10】 電子透かしデータが挿入されたディジタルコンテンツから電子透かしデータを検出するとともに、当該ディジタルコンテンツを表示手段に表示する処理を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体において、

電子透かしが挿入され、かつ、暗号化されたディジタルコンテンツを通信ネットワークから入力し、当該暗号化されたディジタルコンテンツから電子透かしデータを検出する処理と、復号キーを用いて前記暗号化されたディジタルコンテンツを復号する処理と、前記復号されたディジタルコンテンツを再生し、前記表示手段に出力する処理と、前記電子透かしデータと所定のIPアドレスとを前記通信ネットワークに出力する処理と、前記復号キーを前記通信ネットワークから入力する処理とを実行させるためのプログラムを記録した記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、ネットワークを利用したディジタルコンテンツ生成及び再生装置に関し、特にデジタルコンテンツに特殊な情報を持つ識別データ（電子透かしデータ）を挿入後、当該電子透かし入りディジタルコンテンツを暗号化して提供することにより、不正使用者によるディジタルコンテンツの視聴を制限する装置に関する。

##### 【0002】

##### 【従来の技術】

近年、コンテンツのデジタル化が盛んに行われている。コンテンツのデジタル化は、インターネット上のWWW利用者の爆発的増加の効果、大容量データをパーソナルレベルで利用できるハードウェアの普及などにより、一気に加速したといえる。それに伴い、ディジタルコンテンツの違法な複製が大きな社会問題となりつつある。電子透かしデータの挿入・検出技術は、そのような違法な複製

を防止する技術として注目を浴びており、実現化に向けて検討が進んでいる。電子透かし技術とは、デジタルコンテンツのデータそのものに対して、人間が知覚しづらいが機械読みが取り可能なID情報を一種のノイズとして埋め込む技術であり、埋め込まれた情報は、常にデジタルコンテンツとともに存在し、容易には消去や改変ができないという特徴を有する。この特徴を生かしてデジタルコンテンツの不正なコピーを防止することが電子透かし技術の目的である。

## 【0003】

## 【発明が解決しようとする課題】

しかしながら、上述した通り、電子透かし技術とは、デジタルコンテンツのデータそのものに対して、人間が知覚しづらいが機械読みが取り可能なID情報を一種のノイズとして埋め込む技術であるため、電子透かしデータが挿入された画像データ等のデジタルコンテンツは、電子透かしデータが埋め込まれる前のオリジナルのデジタルコンテンツと比べて視聴覚的に遜色はない。したがって、電子透かしデータが挿入されたデジタルコンテンツを格納しているデータ記憶媒体を不正に入手した者であっても、当該コンテンツを視聴することは可能である。

## 【0004】

一方、インターネットが普及するにしたがい、デジタルコンテンツの正当所有者が所定のユーザに対してインターネットを経由して当該デジタルコンテンツを配信するサービスがおこなわれている。

## 【0005】

そこで、本発明では、インターネット又はデータ記憶媒体を使ってデジタルコンテンツを提供する際に、当該デジタルコンテンツに電子透かしデータを挿入するとともに、当該電子透かしが挿入されたデジタルコンテンツを暗号化することにより、不正な使用者の視聴を制限することを目的とする。

## 【0006】

## 【課題を解決するための手段】

かかる目的を達成するために、本発明では、電子透かしデータが挿入されたデジタルコンテンツを所定の暗号キーを使って暗号化し、当該デジタルコンテ

ンツを受信した者は、所定の復号キーを使って当該デジタルコンテンツを復号することによって、視聴する仕組みを提供する。このために、本発明は、デジタルコンテンツ生成装置、デジタルコンテンツ再生装置、及び、デジタルコンテンツ提供システムとから構成される。各装置及びシステムの特徴は次の通りである。

#### 【0007】

本発明のデジタルコンテンツ生成装置の特徴は、電子透かしデータが挿入されたデジタルコンテンツを所定の暗号キーで暗号化して、インターネット上に送出し、又はデータ記憶媒体に格納する点にある。

#### 【0008】

また、本発明のデジタルコンテンツ再生装置の特徴は、電子透かしデータが挿入され、かつ、暗号化されたデジタルコンテンツをインターネット又はデータ記憶媒体から入力し、当該デジタルコンテンツから電子透かしデータを検出するとともに、当該デジタルコンテンツを所定の復号キーで復号化する点にある。

#### 【0009】

さらに、本発明のデジタルコンテンツ提供システムの特徴は、通信回線と、該通信回線と相互に接続されたデジタルコンテンツ再生装置及びデジタルコンテンツ生成装置とを備え、デジタルコンテンツ生成装置は、デジタルコンテンツに電子透かしデータを挿入するとともに暗号化する手段を備え、デジタルコンテンツ再生装置は、電子透かしデータが挿入され、かつ、暗号化されたデジタルコンテンツから電子透かしデータを検出する手段と、当該暗号化されたデジタルコンテンツを所定の復号キーで復号化する手段を含む点にある。

#### 【0010】

尚、参考までに、以下に電子透かし挿入・検出技術の一例を説明するが、本発明は、これに限定されるものではなく、他の電子透かし挿入・検出技術を用いても実現可能である。

#### 【0011】

電子透かし技術の例として、画像を周波数変換し、周波数変換後の映像信号の

周波数成分の強い領域に電子透かしデータを埋め込む方法が提案されている（日経エレクトロニクス 1996. 4. 22 (no. 660) 13ページ）。この方法においては、強い周波数成分に電子透かしデータを埋め込んで、圧縮伸長処理やフィルタリング等の画像処理が施されても、電子透かしデータが失われることはない。この電子透かしデータは、原画像を破壊しない限り、取り除くことはできない。さらに、電子透かしデータとして正規分布に従う乱数を採用することで、電子透かしデータ同士の干渉を防ぎ、電子透かしデータの埋め込みにより、画質が低下することを防止している。

## 【0012】

この方法における電子透かしデータの埋め込み方法は、元の画像をDCT（離散コサイン変換）などを用いて周波数成分に変換し、周波数領域で高い値を示すデータをn個選び、 $f(1)$ 、 $f(2)$ 、 $\dots$ 、 $f(n)$ とし、電子透かしデータ $w(1)$ 、 $w(2)$ 、 $\dots$ 、 $w(n)$ を平均が0分散が1である正規分布より選び、

$$F(i) = f(i) + \alpha \times |f(i)| \times w(i)$$

を各*i*について計算する。ここで $\alpha$ はスケーリング要素である。

## 【0013】

そして、 $F(i)$ に逆DCT変換を施すことにより、電子透かしデータが埋め込まれた画像を得る。

## 【0014】

電子透かしデータの検出は以下の方法で行う。この検出方法においては、元の画像 $f(i)$ 及び電子透かしデータ候補 $w(i)$ （但し*i*=1、2、 $\dots$ 、n）が既知でなければならない。

## 【0015】

まず、電子透かしデータ入り画像をDCT等を用いて周波数成分に変換し、周波数領域において、電子透かしデータを埋め込んだ $f(1)$ 、 $f(2)$ 、 $\dots$ 、 $f(n)$ に対応する要素の値を $F(1)$ 、 $F(2)$ 、 $\dots$ 、 $F(n)$ とする。 $f(i)$ 、及び $F(i)$ により、電子透かしデータ $W(i)$ を

$$W(i) = (F(i) - f(i)) / f(i)$$

により計算して抽出する。

## 【0016】

次に  $w(i)$  と  $W(i)$  の統計的類似度をベクトルの内積を利用して、

$$C = W \cdot w / (WD \times wD)$$

により計算する。ここで、

$$W = (W(1), W(2), \dots, W(n)),$$

$$w = (w(1), w(2), \dots, w(n)),$$

$WD$  = ベクトル  $W$  の絶対値、 $wD$  = ベクトル  $w$  の絶対値、 $\cdot$  はベクトルの内積である。

## 【0017】

統計的類似度  $C$  がある特定の値以上である場合には該当電子透かしデータが埋め込まれていると判定する。

## 【0018】

この方法を用いて電子透かしデータを画像に埋め込んでおけば、原画像を所有している著作者が、違法な複製と思われるデジタル画像データに対して検出処理を行う場合に有効である。この方法は、原画像が必要であるため、違法な複製と思われる画像データに対して原画像を所有している著作者が検出処理を行う場合には電子透かしデータの検出が可能であるが、各端末の再生装置では、原画像がないために電子透かしデータの検出を行うことが出来ない。

## 【0019】

そこでこの方法を改良した方法が提案されている。この方法では、元の画像を  $8 \text{ピクセル} \times 8 \text{ピクセル}$  のブロックに分割し、このブロックを処理単位として、電子透かしデータの埋め込み、及び抽出処理を行う。

## 【0020】

電子透かしデータの埋め込み処理は、まず、DCTが終わった後の周波数領域でAC成分の周波数成分の低いものから順に、 $f(1), f(2), \dots, f(n)$  とすると、電子透かしデータ  $w(1), w(2), \dots, w(n)$  を平均0、分散1である正規分布より選び、

$$F(i) = f(i) + \alpha \times \text{avg}(f(i)) \times w(i)$$

を各  $i$  について計算する。ここで、 $\alpha$  はスケーリング要素であり、 $a v g (f(i))$  は  $f(i)$  の近傍 3 点の絶対値の平均を取った部分平均である。

#### 【0021】

電子透かしデータの検出は以下の方法で行う。この検出方法においては、元の画像は必要ではなく、電子透かしデータ候補  $w(i)$  (但し  $i = 1, 2, \dots, n$ ) が既知であればよい。

#### 【0022】

そして、 $F(i)$  に逆 DCT 変換を施すことにより、電子透かしデータが埋め込まれた画像を得る。

#### 【0023】

電子透かしデータの検出は以下の方法で行う。

#### 【0024】

電子透かしデータが埋め込まれた画像に対して DCT 変換を行い、ブロックの周波数領域の中で周波数成分の低いものから順に、 $F(1), F(2), \dots, F(n)$  とする。 $F(i)$  の近傍 3 点  $F(i-1), F(i), F(i+1)$  の絶対値の平均値を部分平均  $a v g(F(i))$  として、電子透かしデータ  $W(i)$  を  $W(i) = F(i) / avg(F(i))$  により計算し、さらに 1 画像分の  $W(i)$  の総和  $WF(i)$  を  $i$  毎に各々計算する。

#### 【0025】

次に、 $w(i)$  と  $WF(i)$  の統計的類似度をベクトルの内積を利用して、  
 $C = WF \cdot w / (WF D \times w D)$   
 により計算する。統計的類似度  $C$  がある特定の値以上である場合には、該当電子透かしデータが埋め込まれていると判定する。

#### 【0026】

##### 【発明の実施の形態】

本発明のデジタルコンテンツ生成装置の一実施の形態を図面を用いて説明する。

図 1 は、デジタルコンテンツ生成装置の構成を示すブロック図である。

#### 【0027】

本装置は、DVD、CD-ROM等のディスク記録媒体や半導体メディアといったマルチメディアデータを扱うことができるデータ記憶媒体を通じて提供されるディジタルコンテンツ（静止画、動画、音声又はそれらを組み合わせたマルチメディアデータ）の中に、電子透かしデータを挿入し、当該電子透かしが挿入されたディジタルコンテンツを暗号化する装置である。

#### 【0028】

図1を参照すると、本実施形態のディジタルコンテンツ生成装置は、DCT（離散コサイン変換）部101と、電子透かしデータを記憶している電子透かしデータ出力部103と、電子透かしデータ挿入部102と、暗号化部104と、暗号キーを生成する暗号キー生成部105と、復号キーを生成する復号キー生成部106と、インターネットと接続するネットワークインターフェース部107とを備える。また、各構成要素は、パーソナルコンピュータやワークステーションその他のコンピュータシステム上に搭載される情報処理装置及び記憶装置により実現される。情報処理装置は、データを格納するための内部メモリと、信号入力ポートと、信号出力ポートとを有し、かつ、制御プログラムにしたがって処理を実行する。ここで、信号入力ポートは、ディジタルコンテンツが入力されるものであれば良く、信号出力ポートは、暗号化された電子透かし入りディジタルコンテンツを出力するものであれば良い。また、制御プログラムは、磁気ディスクや半導体メモリその他の記憶媒体に格納して提供され、情報処理装置にロードされる。記憶媒体としては、情報処理装置が読み取り可能な媒体であれば良く、特にその形態が制限されることはない。

#### 【0029】

上記構成において、DCT部101は、データ記憶媒体に記憶されている画像等のデータのデータに対して離散コサイン変換を行い、周波数成分信号を電子透かしデータ挿入器102に対して出力する。電子透かしデータ出力部103は、予め、所定の電子透かしデータを格納している。電子透かしデータ挿入部102は、DCT部101からの周波数成分信号と、電子透かしデータ出力部103から出力される電子透かしデータとを受けて、周波数成分信号に対して電子透かしデータを挿入する。暗号キー生成部105は、ディジタルコンテンツを送信する

相手方（ユーザー）のIPアドレス（宛先IPアドレス）と、挿入した電子透かしデータとに基づいて、暗号キーを生成する。尚、この暗号キーの生成アルゴリズムは、一般的には、 $K = F(W, A)$  ( $F$ : 所定の関数、 $K$ : 暗号キー、 $W$ : 電子透かしデータ、 $A$ : IPアドレス) の数式で表されるが、特に、この数式に限定されるものではない。暗号部104は、暗号キーを受けて、その暗号キーを使って電子透かしデータ挿入部102の出力データを暗号化する。ただし、その出力データの先頭に位置するある一定量のデータは暗号化しない。その理由は、後述するように、デジタルコンテンツ再生装置にて電子透かしデータを検出するためである。尚、その暗号化アルゴリズムは、既に知られている一般的なアルゴリズムで構わない。ネットワークインターフェース部107は、暗号部104の出力である暗号化されたデータを、インターネット又はデータ記憶媒体を介して相手方に送る。または、復号キー生成部106に関しては、後述する。

## 【0030】

次に、本発明のデジタルコンテンツ再生装置の一実施の形態を図面を用いて説明する。

図2は、デジタルコンテンツ再生装置の構成を示すブロック図である。

## 【0031】

本装置は、インターネットを通じて提供される暗号化されたデジタルコンテンツの中から電子透かしデータを抽出するとともに、暗号化されたデジタルコンテンツを所定の復号キーを使って復号化し、ディスプレイ等に表示する装置である。

## 【0032】

図2を参照すると、本実施形態のデジタルコンテンツ再生装置は、所定の復号キーを使って、暗号化されたデータを元に戻す復号化部201と、逆DCT部202と、電子透かしデータ検出部203と、ネットワークインターフェイス部204と、再生部205と、表示部206とを備え、装置自身は、インターネットと接続されている。また、本装置には、WWWブラウザがインストールされており、このブラウザが動作するように設定されている。

## 【0033】

また、各構成要素は、パーソナルコンピュータやワークステーションその他のコンピュータシステム上に搭載される情報処理装置、記憶装置及びディスプレイ等の表示装置により実現される。情報処理装置は、データを格納するための内部メモリと、信号入力ポートと、信号出力ポートとを有し、かつ、制御プログラムにしたがって処理を実行する。ここで、信号入力ポートは、暗号化された電子透かし入りデジタルコンテンツが入力されるものであれば良く、信号出力ポートは、デジタルコンテンツ、及び、検出した電子透かしデータを出力することができるものであれば良い。また、制御プログラムは、磁気ディスクや半導体メモリその他の記憶媒体に格納して提供され、情報処理装置にロードされる。記憶媒体としては、情報処理装置が読み取り可能な媒体であれば良く、特にその形態が制限されることはない。

#### 【0034】

上記構成において、復号化部201は、インターネット又はデータ記憶媒体から暗号化された電子透かし入りデータ（例えば、MPEGストリーム形式のデータ）を入力し、電子透かしデータ検出部203及び逆DCT部202に出力する。前述の通り、その電子透かし入りデータの先頭に位置するある一定量のデータは暗号化されていないため、電子透かしデータ検出部203は、電子透かしデータを検出することができる。電子透かしデータ検出部203は、検出した電子透かしデータをネットワークインターフェース部204に出力する。ネットワークインターフェース部204は、自己のIPアドレスと電子透かしデータとをインターネットを経由してデジタルコンテンツ提供装置に送出する。

#### 【0035】

次に、図1に戻って説明する。図1において、復号キー生成部106は、デジタルコンテンツ再生装置が出力した電子透かしデータとIPアドレスとをインターネット経由で入力し、復号キーを生成する。この復号キーは、前述のデジタルコンテンツ再生装置が受信している暗号化されたデジタルコンテンツをを復号化するのに用いるキーである。この復号キーの生成アルゴリズムは、一般的には、 $k = f(W, A)$  ( $f$  : 所定の関数、 $k$  : 復号キー、 $W$  : 電子透かしデータ、 $A$  : IPアドレス) の数式で表されるが、特に、この数式に限定されるも

のではない。尚、秘密鍵暗号方式においては、暗号化と復号化に同じキーを利用する。よって、その方式の場合には、Fとfは同じとなる。このようにして生成された復号キーは、ネットワークインターフェース部107及びインターネットを介して、ディジタルコンテンツ再生装置に送られる。

#### 【0036】

次に、再び図2に戻って説明する。図2において、復号化部201は、ネットワークインターフェース部204から、上記復号キーを受け取り、その復号キーを使って、暗号化されたディジタルコンテンツを復号化し、逆DCT部202に出力する。逆DCT部202は、復号化されたデータを逆離散コサイン変換して再生部205に出力する。再生部205は、ディジタルコンテンツを再生し、表示制御部206に出力する。

#### 【0037】

次に、図3のフローチャートを参照してディジタルコンテンツ生成装置の実施形態の動作について説明する。尚、上述したように本実施形態のディジタルコンテンツ生成装置をコンピュータシステムにて実現する場合、情報処理装置を制御する制御プログラムは、少なくとも以下に説明する各ステップを情報処理装置に実行させる命令を含み、情報処理装置に対して、信号入力ポートから入力されるディジタルコンテンツに電子透かしデータを挿入後、暗号化する処理を行わせる。

#### 【0038】

まず、電子透かしデータ出力部のメモリに、所定の電子透かしデータを記憶する（ステップ301）。次に、信号入力ポートにディジタルコンテンツを入力した後、DCT部101が、入力したディジタルコンテンツに対して離散コサイン変換処理を行う（ステップ302）。次に、電子透かしデータ挿入器102が、DCT部101によりスペクトル変換された結果得られたデータに対して、電子透かしデータ出力部103から得られる電子透かしデータを挿入する（ステップ303）。最後に、暗号化部104は、暗号キー生成部105が電子透かしデータ及びIPアドレスに基づいて作成した暗号キーを使って電子透かしデータ挿入部102の出力データを暗号化する（ステップ304）。一方、上記処理とは

別に、デジタルコンテンツ再生装置から送られてくる電子透かしデータとIPアドレスとに基づいて復号キーを生成して、当該復号キーをデジタルコンテンツ再生装置に送出する。

## 【0039】

次に、図4のフローチャートを参照してデジタルコンテンツ再生装置の実施形態の動作について説明する。尚、上述したように本実施形態のデジタルコンテンツ生成装置をコンピュータシステムにて実現する場合、情報処理装置を制御する制御プログラムは、少なくとも以下に説明する各ステップを情報処理装置に実行させる命令を含み、情報処理装置に対して、信号入力ポートから入力される暗号化された電子透かし入りデジタルコンテンツを復号化する処理を行わせる。

## 【0040】

まず、当該デジタルコンテンツ中の暗号化されていない所定のデータから電子透かしデータを抽出し（ステップ401）、当該電子透かしデータとIPアドレスとをデジタルコンテンツ生成装置に送出する（ステップ402）。一方、復号化部201は、デジタルコンテンツ生成装置から復号キーを受け取り（ステップ403）、当該復号キーを用いてデジタルコンテンツを復号する（ステップ404）。次に、逆DCT部202が、復号化されたデータに対して逆離散コサイン変換処理を行う（ステップ405）。最後に、再生部205及び表示部206が、復号化されたデジタルコンテンツを再生し、ディスプレイに表示する（ステップ406）。

## 【0041】

次に、本発明の記録媒体の実施の形態を図5を用いて説明する。

## 【0042】

図5を参照すると、この実施の形態は、電子透かしの挿入処理と暗号キー発生処理と暗号化処理と復号キー発生処理とを実行するプログラムを記録した記録媒体505を備える。この記録媒体は、磁気ディスク、半導体メモリ等である。このプログラムは記録媒体505から記憶装置502に格納される。データ処理装置503はこのプログラムの制御により、前述の実施の形態と同一の処理を実行

する。すなわち、入力装置501は、データ記憶媒体からデジタルコンテンツを入力し、データ処理装置503に出力する。データ処理装置503は、デジタルコンテンツに電子透かしデータを挿入後、暗号化を行い、出力装置504に出力する。出力装置504は、暗号化されたデジタルコンテンツをインターネットに出力する。また、データ処理装置503は、デジタルコンテンツ再生装置から受け取った電子透かしデータ及びIPアドレスに基づいて復号キーを生成する。

## 【0043】

次に、本発明の記録媒体の実施の形態を図6を用いて説明する。

## 【0044】

図6を参照すると、この実施の形態は、電子透かし抽出処理と復号化処理とを実行するプログラムを記録した記録媒体606を備える。この記録媒体606は、磁気ディスク、半導体メモリ等である。電子透かし挿入プログラムは記録媒体606から記憶装置602に格納される。データ処理装置603は、このプログラムの制御により、前述の実施の形態と同一の処理を実行する。また、データ処理装置603は、デジタルコンテンツの再生処理も実行する。

## 【0045】

すなわち、入出力装置601は、インターネット又はデータ記憶媒体から暗号化されたデジタルコンテンツを入力し、データ処理装置603に出力する。データ処理装置603は、記憶装置602に格納されたプログラムの制御により、デジタルコンテンツから電子透かしデータを検出し、IPアドレスとともに、入出力装置601に出力する。入出力装置601は、当該電子透かしデータとIPアドレスとをインターネットに送出する。また、入出力装置601は、インターネットから復号キーを入力する。データ処理装置603は、入出力装置601から復号キーを受け取り、その復号キーを使って、暗号化されたデジタルコンテンツの復号化を行う。表示装置605は、復号化されたデジタルコンテンツを表示する。

## 【0046】

次に、本発明のデジタルコンテンツ提供システムの実施の形態を図7を用い

て説明する。本システムは、デジタルコンテンツに電子透かしデータを挿入後、暗号化を行う提供者701が保有するデジタルコンテンツ生成装置702と、デジタルコンテンツを再生するユーザ703が保有するデジタルコンテンツ再生装置704とから構成される。

#### 【0047】

デジタルコンテンツ生成装置702は、静止画・動画等のデジタルコンテンツの中に電子透かしデータを挿入した後に、暗号化を行い、その暗号化されたデジタルコンテンツをユーザに提供する装置である。その具体的な構成は、前述の実施の形態で説明した通りである。

#### 【0048】

デジタルコンテンツ再生装置704は、電子透かしデータ入りのデジタルコンテンツを再生し、ディスプレイに表示する装置である。その具体的な構成は、前述の実施の形態で説明した通りである。

#### 【0049】

次に、この実施の形態の動作を説明する。

#### 【0050】

提供者701は、デジタルコンテンツ生成装置を用いて、デジタルコンテンツに電子透かしデータを挿入後、暗号化を行い、その暗号化されたデータをインターネット又はデータ記憶媒体を介して、ユーザが所有しているデジタルコンテンツ再生装置に送る(①)。デジタルコンテンツ再生装置は、電子透かしデータを抽出し、電子透かしデータと自己のIPアドレスとをインターネットを介してデジタルコンテンツ生成装置に送る(②)。デジタルコンテンツ生成装置は、送られてきた電子透かしデータとIPアドレスとに基づいて復号キーを生成し、そのキーをインターネットを介してデジタルコンテンツ再生装置に送る(③)。デジタルコンテンツ再生装置は、そのキーを使って、暗号化されたデータを復号し、再生・表示する。

#### 【0051】

##### 【発明の効果】

本発明では、インターネットを使ってデジタルコンテンツを提供する際に

、当該デジタルコンテンツに電子透かしデータを挿入するとともに、当該電子透かしが挿入されたデジタルコンテンツを暗号化してインターネット上に送出すことにより、不正な使用者の視聴を制限することができる。

【図面の簡単な説明】

【図1】

本発明のデジタルコンテンツ生成装置の一実施の形態を示すブロック図である。

【図2】

本発明のデジタルコンテンツ再生装置の一実施の形態を示すブロック図である。

【図3】

本発明のデジタルコンテンツ生成方法の一実施の形態を示すフローチャートである。

【図4】

本発明のデジタルコンテンツ再生方法の一実施の形態を示すフローチャートである。

【図5】

本発明の記録媒体の一実施の形態を示すブロック図である。

【図6】

本発明の記録媒体の一実施の形態を示すブロック図である。

【図7】

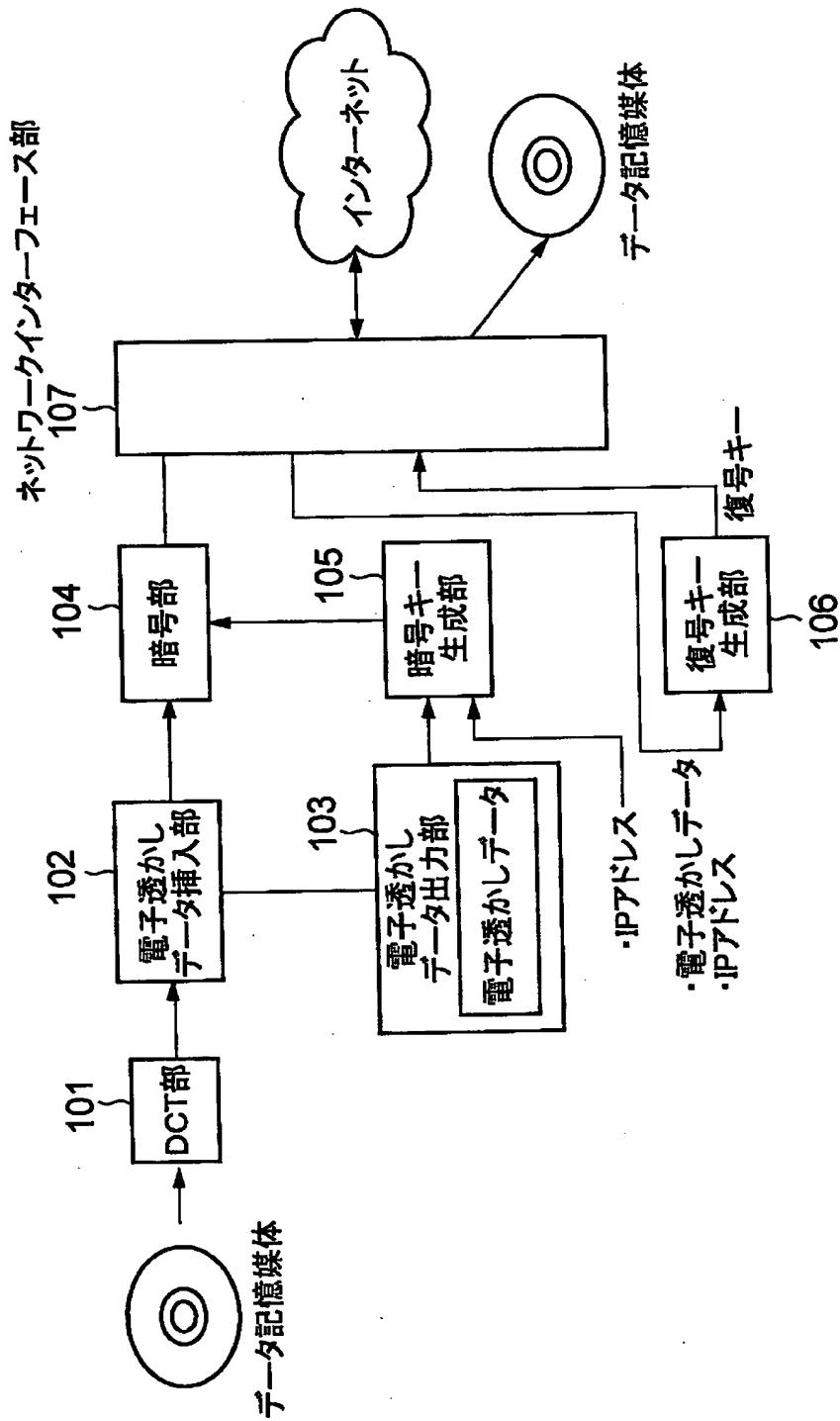
本発明のデジタルコンテンツ提供システムの一実施の形態を示すブロック図である。

【符号の説明】

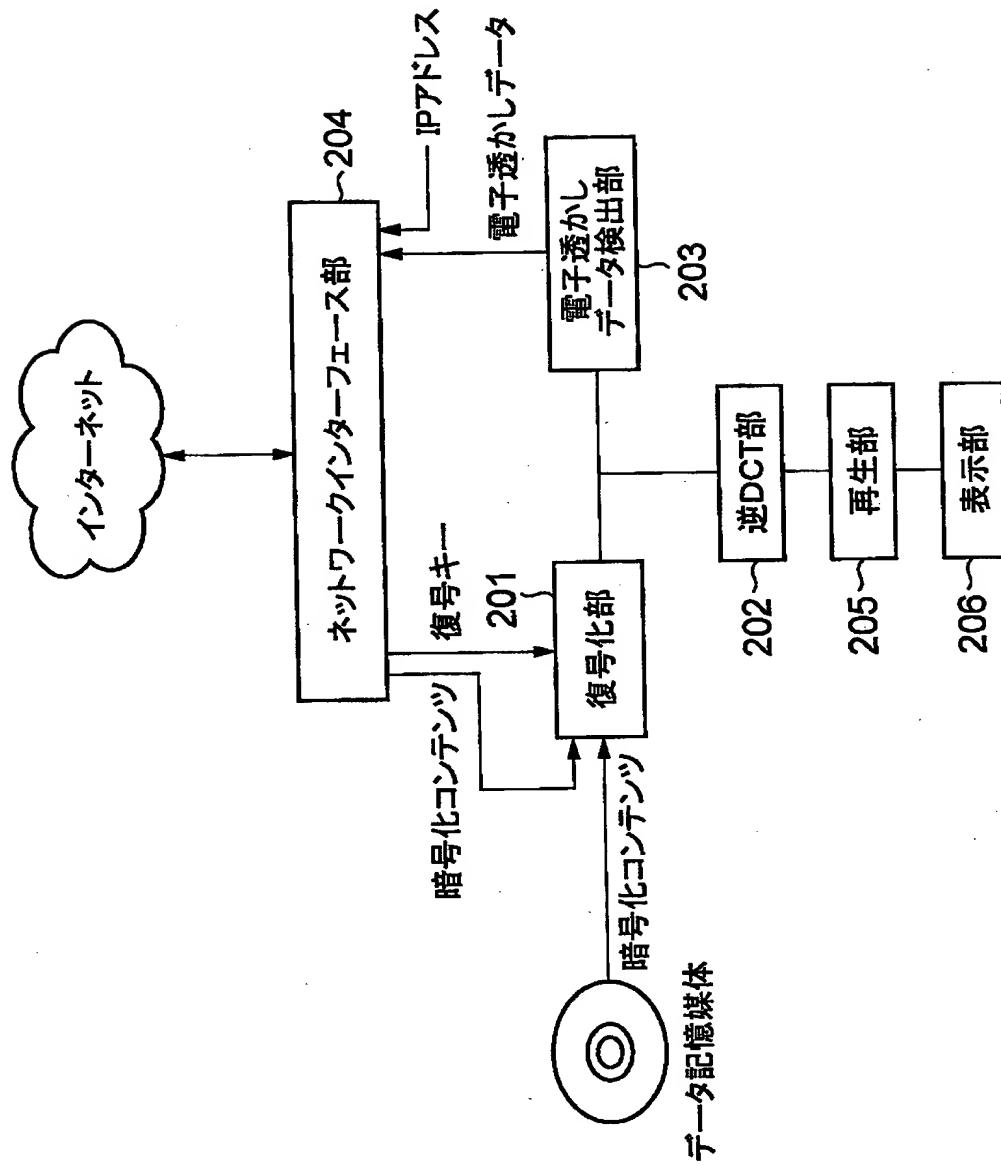
101 DCT部、102 電子透かしデータ挿入部、103 電子透かしデータ出力部、104 暗号部、105 暗号キー生成部、106 復号キー生成部、107 ネットワークインターフェース部、201 復号化部、  
202 逆DCT部、203 電子透かしデータ検出部、204 ネットワークインターフェース部、205 再生部、206 表示部

【書類名】 図面

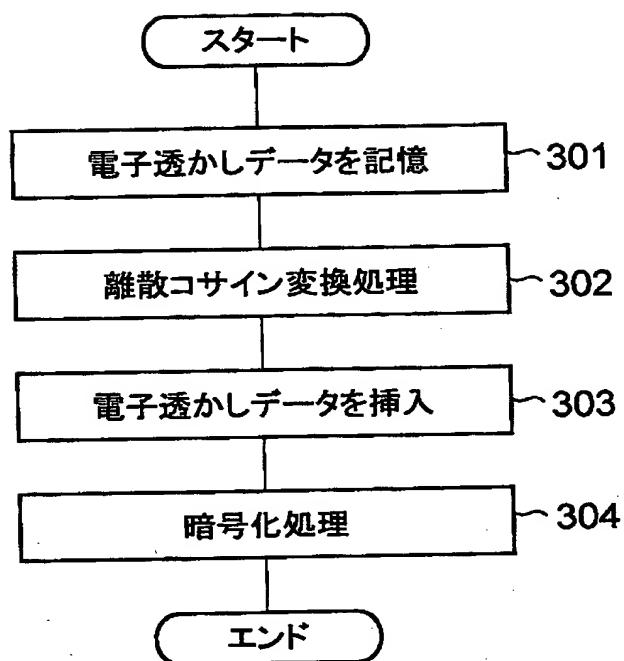
【図1】



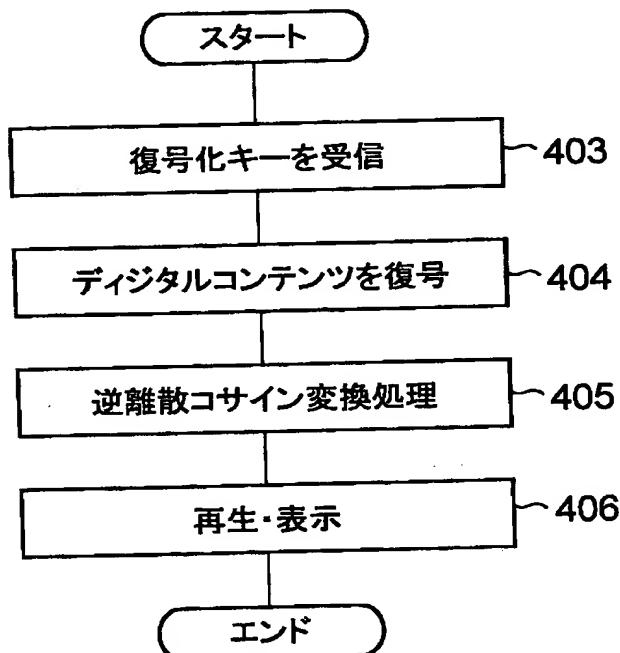
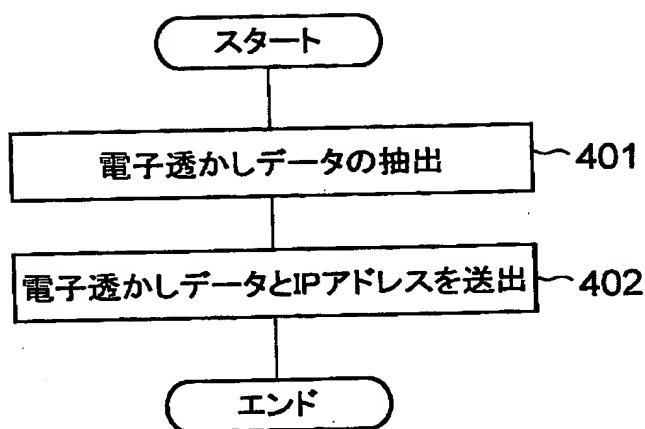
【図2】



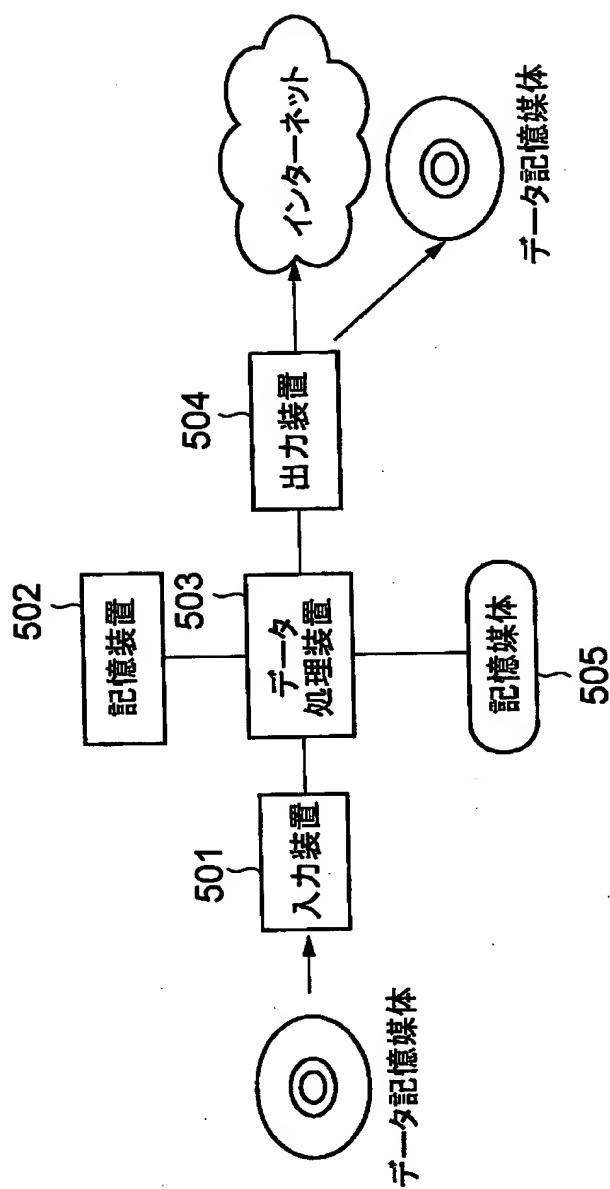
【図3】



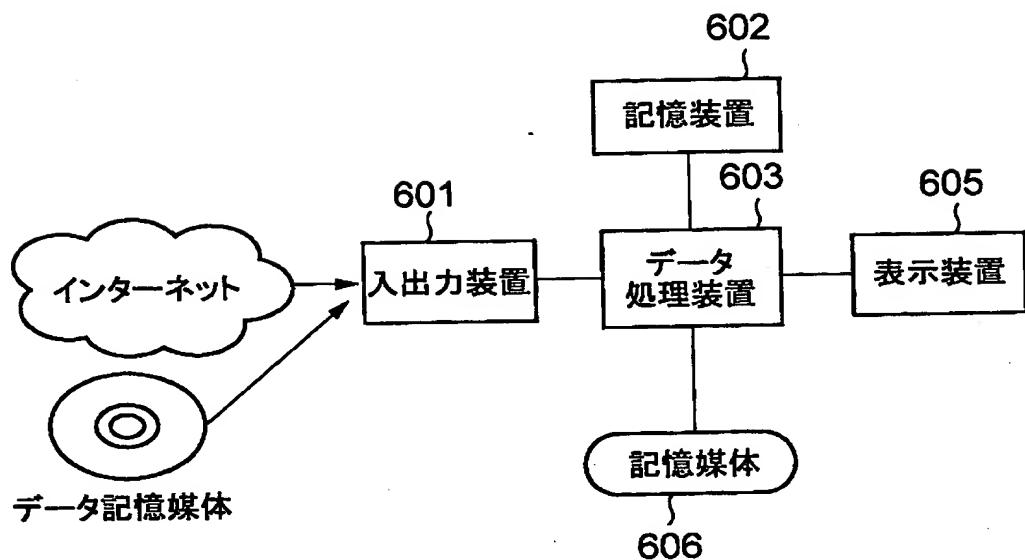
【図4】



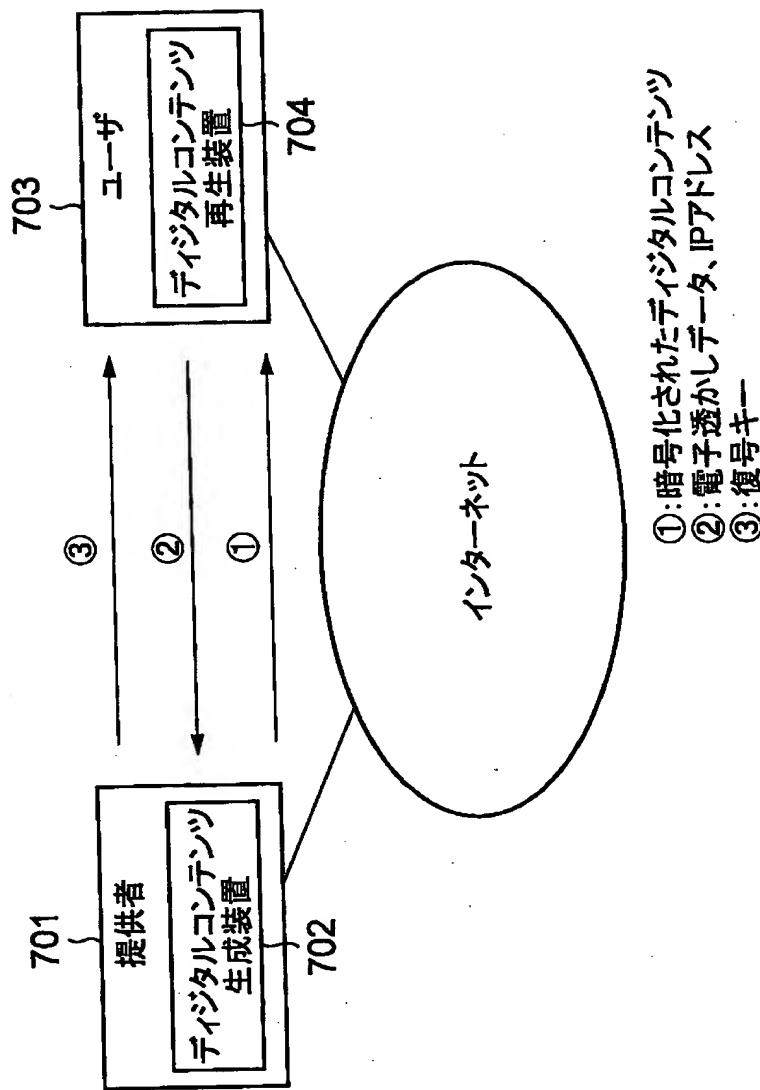
【図5】



【図6】



【図7】



【書類名】 要約書

【要約】

【課題】 インターネットを使ってデジタルコンテンツを提供する際に、当該デジタルコンテンツに電子透かしデータを挿入するとともに、当該電子透かしが挿入されたデジタルコンテンツを暗号化してインターネット上に送出することにより、不正な使用者の視聴を制限する。

【解決手段】 通信回線と、該通信回線と相互に接続されたデジタルコンテンツ再生装置及びデジタルコンテンツ生成装置とを備え、デジタルコンテンツ生成装置は、デジタルコンテンツに電子透かしデータを挿入するとともに暗号化する手段を備え、デジタルコンテンツ再生装置は、電子透かしデータが挿入され、かつ、暗号化されたデジタルコンテンツから電子透かしデータを検出する手段と、当該暗号化されたデジタルコンテンツを所定の復号キーで復号化する手段を含む。

【選択図】 図7

認定・付加情報

特許出願の番号	特願2000-286640
受付番号	50001216021
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 9月22日

<認定情報・付加情報>

【提出日】 平成12年 9月21日

次頁無

出願人履歴情報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 東京都港区芝五丁目7番1号

氏 名 日本電気株式会社